AMENDMENTS TO THE SPECIFICATION

Please amend Paragraph [0029] of the specification to reflect the following indicated below.

[0029] FIG. 2 is a flowchart of an example embodiment of the process for obtaining a token 130 in the present invention. As previously discussed, a token 130 may be, but not limited to, a smart card or other device capable of storing and utilizing PKI certificates/private keys. Processing begins in operation 200 and immediately proceeds operation 210. In operation 210, token 130 is loaded with a unique key used for wrapping certificates/private keys which may comprise public and private keys as well as encryption certificates/private keys, signature certificates, and role certificates. This wrapping of certificates/private keys serves the function of encrypting and thereby protecting all items contained within the token 130 from individuals who do not have the associated passphrase. Processing then proceeds to operation 220 where the secret/private key in the key pair generated in operation 210 is stored in the token 130. As will be discussed in further detail in reference to FIGS. 3 and 4, it is not necessary for a user to utilize a secure computer system to utilize and update the token 130 due to this wrapping of certificates/private keys utilizing the aforementioned wrapping key. In operation 230, the user's identity and credentials are verified by a personal registration authority 146. This personal registration authority 146 may be a badge or security officer. ~~Thereafter,~~In operation 240, the personal registration authority 146 signs a request, which is an

electronic form, comprising the users identification, token identification and organizational code. The token identification is embedded in each token during the manufacturing process and is a unique identifier. This information is transmitted to the certificate authority 110. In operation 250, the certificate authority 110 checks for redundant tokens 130 assigned to this user and revokes the same. In operation 260, the electronic form is filed with the certificate authority 110 from the users organizational database. In operation 270, the personal registration authority 146 signs and submits the electronic form after review of the data against the credentials supplied by the user 132. Processing then proceeds to operation 280 where the certificate authority 110 validates the personal registration 146 signature certificate. Operation 280 serves to verify the identity of the personal registration authority 146 and prevents tokens from being issued by unauthorized individuals. Processing then proceeds to operation 290 where all encryption, signature, and role certificates are generated by the certificate authority 110 and wrapped in the token 130 public key. This wrapping function serves to encrypt the certificates/private keys in order to prevent interception by unauthorized individuals. Thereafter, in operation 300 the token 130 may unwrap the certificates/private keys received using its private key and thereby activating the certificates/private keys. Only the token 130 having a private key that matches the public key is able to open a certificate/private key and activate them. Further, a passphrase may be required by the token 130 prior to attempting to open a certificate/private key. Processing then proceeds to operation 310 where processing terminates.